

## I Claim:

- 1 1. A system of encrypting and decrypting data using private keys for  
2 secure transmission, comprising:  
3 an encrypt and decrypt engine for encrypting and decrypting data  
4 with a private key using associative properties of encrypting and  
5 decrypting, wherein said encrypt and decrypt engine can encrypt an  
6 unsecured data file with a first private key into a first encrypted file,  
7 encrypt the first encrypted data file with a second private key into a  
8 second encrypted file, decrypt the second encrypted file with the first  
9 private key into a third encrypted file, and decrypt the third encrypted  
10 file with the second private key into the unsecured data file.
- 1 2. The system of claim 1, wherein the private keys contain biometric  
2 data identifying its user.

1 3. A method of encrypting, decrypting and transmitting data using  
2 private keys for secure transmission from a first computer to a second  
3 computer, comprising the steps of:  
4 providing unsecured data for transmission at the first computer;  
5 encrypting the unsecured data using a first private key into a first  
6 encrypted data file;  
7 transmitting the first encrypted data file to the second computer;  
8 encrypting the first encrypted data file using a second private key  
9 into a second encrypted data file;  
10 transmitting the second encrypted data file to the first computer;  
11 decrypting the second encrypted data file using the first private key  
12 into a third encrypted data file;  
13 transmitting the third encrypted data file to the second computer;  
14 and  
15 decrypting the third encrypted data file using the second private  
16 key into the unsecured data.

1 4. The method of claim 3, further including the step of storing the  
2 unsecured data on the second computer.

1 5. The method of claim 3, further including the step of verifying the  
2 validity of the unsecured data after decrypting the third encrypted data  
3 file at the second computer.

1 6. The method of claim 3, wherein the encrypting and decrypting is  
2 performed using associative properties of encryption and decryption.

1 7. The method of claim 3, wherein the private keys can include  
2 digitized biometric data identifying its user.

1 8. The method of claim 3, further including the step of processing the  
2 unsecured data after decrypting the third encrypted data file at the  
3 second computer.

1 9. A method of encrypting and decrypting data using private keys for  
2 secure transmission from a first computer to a second computer,  
3 comprising the steps of:

4 encrypting unsecured data using a first private key into a first  
5 encrypted data file at the first computer;

6 encrypting the first encrypted data file using a second private key  
7 into a second encrypted data file at the second computer;

8 decrypting the second encrypted data file using the first private key  
9 into a third encrypted data file at the first computer; and

10 decrypting the third encrypted data file using the second private  
11 key into the unsecured data at the second computer.

1 10. The method of claim 9, further including the step of storing the  
2 unsecured data on the second computer.

1 11. The method of claim 9, further including the step of verifying the  
2 validity of the unsecured data after decrypting the third encrypted data  
3 file at the second computer.

1 12. The method of claim 9, wherein the encrypting and decrypting is  
2 performed using associative properties of encryption and decryption.

1 13. The method of claim 9, wherein the private keys can include  
2 digitized biometric data identifying its user.

1 14. The method of claim 9, further including the step of processing the  
2 unsecured data after decrypting the third encrypted data file at the  
3 second computer.

1 15. A computer-readable medium comprising program instructions for  
2 encrypting and decrypting data using private keys for secure  
3 transmission from a first computer to a second computer, comprising the  
4 steps of:

5 encrypting unsecured data using a first private key into a first  
6 encrypted data file at the first computer;

7 encrypting the first encrypted data file using a second private key  
8 into a second encrypted data file at the second computer;

9 decrypting the second encrypted data file using the first private key  
10 into a third encrypted data file at the first computer; and

11 decrypting the third encrypted data file using the second private  
12 key into the unsecured data at the second computer.

- 1 16. The method of claim 15, wherein the encrypting and decrypting is
- 2 performed using associative properties of encryption and decryption.

005250" 00455560